



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,002	07/05/2001	Mark J. McArdle	002114.P020	5144
28875	7590	05/12/2005	EXAMINER	
Zilka-Kotab, PC P.O. BOX 721120 SAN JOSE, CA 95172-1120			PWU, JEFFREY C	
		ART UNIT		PAPER NUMBER
				2143

DATE MAILED: 05/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)	
	09/900,002	MCARDLE ET AL.	
	Examiner	Art Unit	
	Jeffrey C. Pwu	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 28 February 2005.

2a) This action is **FINAL**.                                   2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-29 is/are pending in the application.

4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5) Claim(s) \_\_\_\_\_ is/are allowed.

6) Claim(s) 1-29 is/are rejected.

7) Claim(s) \_\_\_\_\_ is/are objected to.

8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All    b) Some \* c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_

4) Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_

5) Notice of Informal Patent Application (PTO-152)

6) Other: \_\_\_\_\_

## **DETAILED ACTION**

### ***Claim Rejections - 35 USC § 112***

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 26 recites the limitation "DNS service" in claim 24. There is insufficient antecedent basis for this limitation in the claim.
3. Claim 27 is rejected for incorporating the defects from the parent claim by dependency.

### ***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-25, and 28-29 are rejected under 35 U.S.C. 102(b) as being anticipated by Ginter et al. (U.S. 5,892,900).

Ginter et al. disclose claims :

1. A computerized method for restricting network access by applications comprising:

- detecting a network access request from an application;
- examining an application policy file (fig. 2A, "rules and controls"; fig. 5A, 808, "permissions record") to determine if the application is authorized to access the network by comparing an identifier for the application with identifiers in the application policy file that correspond to applications authorized for installation on computers coupled to the network ("virtual distribution environment"-VDE; "secures, administers, and audits electronic information use. VDE also features fundamentally important capabilities for managing content that travels "across" the "information highway." These capabilities comprise a rights protection solution that serves all electronic community members. These members include content creators and distributors, financial service providers, end-users, and others. VDE is the first general purpose, configurable, transaction control/rights protection solution for users of computers, other electronic appliances, networks, and the information highway."); method steps of figs. 69A-69M); and
- blocking access to the network if the application is not authorized to access the network. (fig.69K; method steps 3564-3574)

2. The method of claim 1 further comprising: determining a network resource requested by the application; examining the application policy file to determine if the application is authorized to access the network resource; and allowing access to the network resource if the application is authorized to access the network resource. (see "Document Control Policies"; col.302, line 40-col.303, line 39);

3. The method of claim 1 further comprising: determining a type of network access requested by the application; examining the application policy file to determine if the application is authorized for the type of network access requested; and allowing the type of network access requested if the application is authorized for the type of network access requested. (col.302, line 40-col.303, line 39)
4. The method of claim 1 further comprising: updating the application policy file; and re-evaluating applications currently executing against the updated policy file. (col.302, line 40-col.303, line 39)
5. The method of claim 1, wherein the application identifier is in the network access request. (figs. 5A, 5B)
6. The method of claim 1, wherein the method is performed on a client computer on which the application is executing. (112)
7. A computer-readable medium having executable instruction to cause a computer to perform a method comprising: detecting a network access request from an application; examining an application policy file to determine if the application is authorized to access the network by comparing an identifier for the application with identifiers in the application policy file that correspond to applications authorized for installation on

computers coupled to the network; and blocking access to the network if the application is not authorized to access the network. (claim 7 is similarly rejected as in claim 1)

8. The computer-readable medium of claim 7, wherein the method further comprises: determining a network resource requested by the application; examining the application policy file to determine if the application is authorized to access the network resource; and allowing access to the network resource if the application is authorized to access the network resource. (claim 8 is similarly rejected as in claims 1-6)

9. The computer-readable medium of claim 7, wherein the method further comprises: determining a type of network access requested by the application; examining the application policy file to determine if the application is authorized for the type of network access requested; and allowing the type of network access requested if the application is authorized for the type of network access requested. (claim 9 is similarly rejected as in claims 1-6)

10. The computer-readable medium of claim 7, wherein the method further comprises: updating the application policy file; and re-evaluating applications currently executing against the updated policy file. (claim 10 is similarly rejected as in claims 1-6)

11. The computer-readable medium of claim 7, wherein the application identifier is in the network access request. (claim 11 is similarly rejected as in claims 1-6)

12. A computer system comprising:

a processing unit; a memory coupled to the processing unit through a bus; a network interface coupled to the processing unit through the bus and further operable for coupling to a network; and an application policy process executed from the memory by the processing unit to cause the processing unit to detect a network access request from an application, to examine an application policy file to determine if the application is authorized to access the network by comparing an identifier for the application with identifiers in the application policy file that correspond to applications authorized for installation on computers coupled to the network, and to block access to the network if the application is not authorized to access the network. (claim 12 is similarly rejected as in claim 1)

13. The computer system of claim 12, wherein the application policy process further causes the processing unit to determine a network resource requested by the application, to examine the application policy file to determine if the application is authorized to access the network resource, and to allow access to the network resource if the application is authorized to access the network resource. (claim 13 is similarly rejected as in claims 1-6)

14. The computer system of claim 12, wherein the application policy process further causes the processing unit to determine a type of network access requested by the

application, to examine the application policy file to determine if the application is authorized for the type of network access requested, and to allow the type of network access requested if the application is authorized for the type of network access requested. (claim 14 is similarly rejected as in claims 1-6)

15. The computer system of claim 12, wherein the application policy process further causes the processing unit to update the application policy file, and to re-evaluate applications currently executing against the updated policy file. (see "Document Control Policies")

16. The computer system of claim 12, wherein the application identifier is in the network access request. (claim 16 is similarly rejected as in claims 1-6)

17. The computer system of claim 12, wherein the application is executed from the memory by the processing unit. (502 or 620)

18. A computer-readable medium having stored thereon an application policy data structure comprising: an application identifier field containing data identifying an application that is authorized for installation on computer coupled to a network; a network identifier field containing data identifying a entity that is accessible by the application identified by the application identifier field; and an access flag field containing data specifying whether the application identified by the application identifier

field is allowed access to the entity identified by the network identifier field. (claim 18 is similarly rejected as in claim 1; col.12, line 45- col.13, line 67)

19. The computer-readable medium of claim 18 further comprising: an additional policy rule field containing data specifying whether the application identified by the application identifier field is allowed a particular type of access to the entity identified by the network identifier field. (col.3, line 18-col.13, line 67)

20. The computer-readable medium of claim 18 further comprising: a response field containing data specifying an action to be performed if the application identified by the application identifier field attempts access to the entity identified by the network identifier field and the access is not allowed. (col.3, line 18-col.13, line 67)

21. The computer-readable medium of claim 18, wherein the entity is selected from the group consisting of a network and a network resource. (col.3, line 18-col.13, line 67)

22. The method of claim 5, wherein the application identifier is selected from the group consisting of a file name of the application and a path on the network. (col.3, line 18- col.13, line 67)

23. The method of claim 5, wherein a plurality of the application identifiers are associated with each application, and each of the application identifiers corresponds to

a different network address assigned to the corresponding application. (col.3, line 18-col.13, line 67)

24. The method of claim 1, wherein each application entry in the application policy file comprises a set of access policy rules for one of a network and a network resource identified by a network identifier. ("Document Control Policies" and col.302, line 40-col.303, line 39)

25. The method of claim 24, wherein the network identifier is selected from the group consisting of a network address range and a Universal Naming Convention path. (col.3, line 18-col.13, line 67)

28. The method of claim 1 wherein the application policy file includes an application identifier, a network identifier, an access flag, additional policy rules, and at least one application entry. (col.302, line 40-col.303, line 39)

29. A computerized method for execution on a computer coupled to a network to restrict network access by an application executing on the computer, the method comprising: detecting a network request from the application, the request comprising at least one of an identifier and entity and a type of network access, wherein the entity is one of a network and a network resource; examining an application policy file to determine if the application is authorized to access the entity by comparing an identifier for the

application with identifiers in the application policy file that correspond to applications authorized for installation on computers coupled to the network, wherein each application entry in the application policy file comprises a set of access policy rules for a network corresponding to a network identifier, the network identifier comprising at least one of a network address range and a Universal Naming Convention path, and wherein the application policy file further comprises an access flag having a null setting that is interpreted as one of allowing and disallowing all access to a network specified by the network identifier; blocking access to the entity if the application is not authorized to access the entity; and re-evaluating applications currently executing against any updated application policy file, wherein a plurality of the application identifiers are associated with each application, each application identifier corresponding to a different network address assigned to the corresponding application, and wherein each application identifier is one of a file name of the application and a path on the network.

(Claim 29 is similarly rejected as in claims 1-25)

***Response to Arguments***

6. Applicant's arguments with respect to claims 1-29 have been considered but are moot in view of the new ground(s) of rejection.

***Conclusion***

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey C. Pwu whose telephone number is 571-272-6798. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Wiley can be reached on 571-272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



5/10/05

JEFFREY PWU  
PRIMARY EXAMINER